THEODORE J. BOUTROUS, JR. (SBN 132099)
tboutrous@gibsondunn.com
JOSHUA A. JESSEN (SBN 222831)
jjessen@gibsondunn.com
JEREMY S. SMITH (SBN 283812)
jssmith@gibsondunn.com
LAUREN M. BLAS (SBN 296823)
lblas@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

MICHAEL LI-MING WONG (SBN 194130)
mwong@gibsondunn.com
RACHEL S. BRASS (SBN 219301)
rbrass@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

ANN MARIE MORTIMER (SBN 169077)
amortimer@huntonAK.com
JASON J. KIM (SBN 221476)
kimj@huntonAK.com
KIRK A. HORNBECK (SBN 241708)
khornbeck@huntonAK.com
HUNTON ANDREWS KURTH LLP
550 South Hope Street, Suite 2000
Los Angeles, CA 90071
Telephone: 213.532.2000
Facsimile: 213.532.2020

SAMUEL A. DANON (admitted *pro hac vice*)
sdanon@huntonAK.com
JOHN J. DELIONADO (admitted *pro hac vice*)
jdelionado@huntonAK.com
HUNTON ANDREWS KURTH LLP
1111 Brickell Avenue, Suite 2500
Miami, Florida 33143
Telephone: 305.810.2500
Facsimile: 305.810.2460

Attorneys for Defendants YAHOO! INC. and
AABACO SMALL BUSINESS, LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: YAHOO! CUSTOMER DATA
SECURITY BREACH LITIGATION

CASE NO. 16-MD-02752-LHK

DEFENDANTS YAHOO! INC. AND AABACO SMALL BUSINESS, LLC'S OPPOSITION TO PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

Hearing:

Date:	November 1, 2018
Time:	1:30 p.m.
Place:	Courtroom 8 – 4th Floor
Judge:	Hon. Lucy H. Koh

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

I. Summary of Argument and Issues to Be Decided

The most "important[]" and "critical question" for class certification under Rule 23(b)(3) is "whether common evidence and common methodology could be used to prove the *elements* of the underlying cause of action." *Davidson v. Apple Inc.*, 2018 WL 2325426, at *14 (N.D. Cal. May 7, 2018) (emphasis added) (citing *Amgen Inc. v. Conn. Ret. Plans & Tr. Funds*, 568 U.S. 455, 459-60 (2013)). Plaintiffs flunk that test for two simple reasons: each of the claims Plaintiffs seek to certify requires them to prove—not merely allege—(1) that they were *harmed* by one of the cyberattacks on Yahoo, and (2) that Yahoo's actions *caused* that harm. *See* CACI 303 ("To recover," the plaintiff "must prove" that he or she "was harmed" and that the "breach of contract was a substantial factor in causing [his or her] harm"); CACI 400 (the plaintiff "must prove" he or she "was harmed" and that the "negligence was a substantial factor in causing [his or her] harm"); Cal. Civ. Code § 1798.84 ("Any customer *injured by a violation* of this title may institute a civil action to recover damages." (emphasis added)). Discovery has revealed that Plaintiffs have no classwide proof of those elements and that proving each one would require potentially millions of mini-trials.

Plaintiffs propose two models that purport to establish that each class member suffered a common economic harm that Yahoo allegedly caused: (1) a "Lost Value of Personal Identifying Information ('PII')" model, and (2) an "Identity Theft Losses" model. Mot. for Class Certification ("Mot.") at 26-27, 30. Neither model actually offers common proof. Take Plaintiff Paul Dugas, for example. For one of his Yahoo accounts, there was *no* actual PII stored on any Yahoo server, either in Yahoo's user database or in his email account. Yet, Plaintiffs' proposed "Lost Value of PII" model would find that he was injured in the same way as someone with an account containing current, accurate information in Yahoo's user database *and* sensitive PII in her email.

Or take Plaintiff Kimberly Heines. She alleges that *because* Yahoo was infiltrated three times by highly sophisticated cyber criminals from 2013 to 2016, she was the victim of certain fraudulent charges on her debit card. ECF 196 ¶ 18. But discovery has conclusively *ruled out* the attacks on Yahoo as a cause of the debit card fraud because the information needed to commit the crime could not possibly have been taken from Yahoo or from Ms. Heines's Yahoo email account. Ferrante Rpt. at 25-26. Rather, the perpetrator likely captured and cloned her debit card using a card "skimmer" at a gas station or other merchant. *Id.* A reliable means of proof therefore excludes Ms. Heines from recovering, but Plaintiffs' "Identity Theft Losses" model not only fails to capture these indisputable facts, but would ride roughshod over Yahoo's ability to present this and other individualized defenses to the jury, in violation of due process. *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 367 (2011).

These are just two examples of the millions of unavoidable individual, testimony-intensive inquiries necessary to (1) isolate who was actually harmed by conduct attributable to Yahoo (*Moore v. Apple Inc.*, 309 F.R.D. 532, 542-43 (N.D. Cal. 2015)), and (2) preserve Yahoo's constitutional right to present its causation and harm evidence to the jury (*Dukes*, 564 U.S. at 350). Moreover, Plaintiffs admittedly cannot "isolat[e] the damages attributable to Defendant's alleged wrongdoing," as the law requires. *Werdebaugh v. Blue Diamond Growers*, 2014 WL 7148923, at *11 (N.D. Cal. Dec. 15, 2014) (citing *Comcast Corp. v. Behrend*, 569 U.S. 27, 35 (2013)).

Plaintiffs' proposals for Rule 23(b)(2) and (c)(4) certification are similarly flawed. None of the Named Plaintiffs can adequately represent a class seeking injunctive relief because none can prove that they will be reinjured (to the extent they were injured at all) by any conduct attributable to Yahoo, much less that such a threat of reinjury is "immediate." *Chapman v. Pier 1 Imports (U.S.) Inc.*, 631 F.3d 939, 946 (9th Cir. 2011) (en banc). Equally unworkable is their proposal to certify ten issues under Rule 23(c)(4); such certification would not "significantly advance the resolution of the underlying case," and thus is improper under this Court's and the Ninth Circuit's jurisprudence. *Valentino v. Carter-Wallace, Inc.*, 97 F.3d 1227, 1229 (9th Cir. 1996); *Davidson*, 2018 WL 2325426, at *14.

The Court should deny Plaintiffs' motion for class certification in its entirety.

II. Background

A. Cybercriminals Attack Yahoo's Systems

From 2013 to 2016, Yahoo was repeatedly attacked by a veritable "who's who" of cybercriminals. With Yahoo's assistance and cooperation, the U.S. Department of Justice determined that the Federal Security Service ("FSB")—the successor agency to the infamous "KGB"—perpetrated two of the three attacks (referred to by Plaintiffs as the "2014 Breach" and the "Forged Cookie Breach") and a federal grand jury in this District indicted several Russian government officials for cybercrimes. *See* Decl. of Joshua Jessen, Ex. 88 ¶¶ 1, 21, 26-28 [criminal indictment]; ECF 257-1 at YMDL008625923

[SEALED].[1] Federal officials still have not charged anyone in connection with the 2013 attack (referred to by Plaintiffs as the "2013 Breach"). Ex. 36 (Zadig Dep.) at 383:14-384:10.

1. The 2013 Attack

In 2013, cybercriminals [redacted]. Tepstein Decl. Ex. 6 at 7. That database [redacted]. ECF 250-10 at YMDL008625972 [SEALED]. The database does not, however, contain [redacted]. Tepstein Decl. Ex. 5 at 6. At that time, [redacted] (Chhabra Decl. ¶ 12), and for some of it ([redacted], the white pages of a phone book are likely a more reliable resource.

Yahoo did not discover this attack until [redacted]. Tepstein Decl. Ex 6 at 3; Ex. 36 (Zadig Dep.) at 106:6-15. Even today, neither Stroz Friedberg (the forensic firm engaged to investigate the attack) nor the federal government [redacted] Tepstein Decl. Ex. 6 at 7-8; Ex. 36 (Zadig Dep.) at 383:14-384:10.

2. The 2014 Attack

In 2014, Yahoo suffered another attack, this time by known Russian agents and the FSB. Ex. 88 ¶ 21 [criminal indictment]. [redacted]. Tepstein Decl. Ex. 8 at 2-3, 12; *id.* Ex. 5 at 6; Ex. 88 ¶ 15 [criminal indictment]. One of the responsible hackers was Alexsey Belan—one of the FBI's "Most Wanted" hackers since 2012. Ex. 88 ¶ 4 [criminal indictment].

The attackers [redacted]). Tepstein Decl. Ex. 5 at 1-2. They used this information to [redacted]

[1] Unless otherwise noted, all exhibits are attached to the concurrently filed Jessen Declaration.

[redacted], and Alexandra Chalupa, a Democratic National Committee consultant who researched President Trump's hire of Paul Manafort.[2] *See id.*, Ex. 7 at 22; Ex. 88 ¶¶ 34, 36 [criminal indictment]; ECF 252-5 [SEALED]; Michael Isikoff, *Exclusive: Suspected Russian hack of DNC widens — includes personal email of staffer researching Manafort*, Yahoo! (July 25, 2016), https://www.yahoo.com/news/exclusive-hacked-emails-of-dnc-oppo-researcher-point-to-russians-and-wider-penetration-154121061.html.

3. The "Forged Cookie" Attack

While investigating the 2014 attack, Yahoo discovered [redacted] *See* Tepstein Decl. Ex. 7 at 13, 18. There is no evidence that a fraudulent cookie was made (much less used) for any of the Named Plaintiffs (Chhabra Decl. ¶ 3), and no Named Plaintiffs have evidence they received individual notice of the Forged Cookie attack.

B. The Information Stolen From Yahoo's User Database

The criminals obtained [redacted] Tepstein Decl. Ex 6 at 10; *id.*, Ex. 5 at 1-2. The accuracy and completeness of the information within, however, depended largely on what each individual user chose to provide. Some provided [redacted]; others provided merely a [redacted]. Whipple Decl. ¶ 5. Some provided [redacted] *Id.* Some had multiple accounts and provided [redacted] or one account, [redacted] for another account. *Id.* Some had [redacted] at the time of the attacks, [redacted]. *Id.* ¶ 5; *infra* at Fig. 2.

The information on the Named Plaintiffs [redacted] illustrates this. Tepstein Decl. Ex. 6 at 7. For example, Plaintiffs Kimberly Heines, Matthew Ridolfo, and Deana Ridolfo provided [redacted], so the database included that information. Whipple Decl. Ex. 10.

[2] Plaintiffs' references to the timing of Yahoo's disclosure of the 2014 attack relates only to the claim brought by the California subclass under the California Customer Records Act. Mot. at 10-12.

By contrast, Plaintiff Yaniv Rivlin provided only his country. *Id.* The completeness and accuracy of birthday input was similarly varied: Plaintiff Essar (who was born in 1978) provided a fake birthdate [redacted] in connection with his [redacted] account. *Id.*; Ex. 49 (Essar Dep.) at 8:6-7. Plaintiff Deana Ridolfo provided the birthdate of her *husband*, Plaintiff Matthew Ridolfo, not her own, while he provided his own birthdate. Ex. 80 (M. Ridolfo Dep.) at 8:10-11; Ex. 77 (D. Ridolfo Dep.) at 7:14-16; Whipple Decl. Ex. 10.

Certain Named Plaintiffs had multiple accounts and provided different information across them. For example, Plaintiff Paul Dugas provided a real name and birthdate in connection with his [redacted] account, but a fake name and birthdate in connection with his [redacted] account. Ex. 37 (Dugas Dep.) at 13:14-15; Whipple Decl. Ex. 10. Ms. Granot provided a fake name [redacted] a fake birthdate [redacted] and a fake and incomplete address ([redacted] in connection with her [redacted] account, but she provided her real birthdate, first name, and country for her [redacted] account. Ex. 52 (Granot Dep.) at 9:6-8, 7:23-8:13; Whipple Decl. Ex. 10. Plaintiff Andrew Mortensen provided a real address, telephone number, and birthdate in connection with his [redacted] account, but did not provide a full address or telephone number in connection with his [redacted] account. Ex. 60 (Mortensen Dep.) at 11:5-8; 36:14-38:5; 108:25-110:20; Whipple Decl. Ex. 10. Other information in the database was accurate at the time of entry, but outdated by the time of the attacks. For example, the address for Ms. Heines's account was already outdated by the time of the 2013 attack. Ex. 55 (Heines Dep.) at 34:16-36:19; Whipple Decl. Ex. 10.

C. Potentially Accessible Information in Emails

Because the stolen copies of the user database included usernames and passwords, criminals had the opportunity to try to break the hash on those passwords to access the contents of a particular Yahoo user's email—provided, of course, that the user had an email account. Ferrante Rpt. at 5; Chhabra Decl. ¶¶ 6-9. But the type of information accessible in the emails varied because usage varies from person to person. Tucker Rpt. ¶¶ 23-26. For example, Mr. Neff and Mr. Mortensen used their Yahoo accounts for all communications and sent PII through them regularly (despite warnings from Yahoo not to do so). Ex. 71 (AMORTENSEN000094-96); Ex. 70 (AMORTENSEN002442-43); Ex. 75

(Neff001426-45). Others rarely or never sent PII through their Yahoo email. Ms. Granot used her [redacted] account only to receive "silly" or "promotional" emails, and sent no personal information. Ex. 52 (Granot Dep.) at 40:23-41:13. Ms. Ridolfo testified that she used her Yahoo account for the last 17 years "strictly" for online shopping and the like. Ex. 77 (D. Ridolfo Dep.) at 37:8-38:8. And Mr. Rivlin had documents showing he frequently transmitted sensitive information through his Gmail account, but only two instances of sending such information through his Yahoo account. Ex. 84 (Rivlin Dep.) at 53:8-54:9; 57:12-23; 59:25-60:9; 75:1-76:3; 110:6-111:17.

Still other Named Plaintiffs had multiple Yahoo email accounts, each used each for different purposes and each containing different kinds of information. For instance, Mr. Dugas had three different Yahoo email accounts during the relevant time frame. He used the [redacted] account to communicate with other diesel vehicle "enthusiasts" and to purchase parts; used [redacted] for business and personal correspondence; and used [redacted] primarily for personal reasons and "occasionally" for business. Ex. 37 (Dugas Dep.) at 73:10-74:4; *see also id*. at 59:4-25; 71:10-72:11; 59:4-14; 68:10-69:6. He testified that he "probably" transmitted financial information through emails in some, but not all accounts, but produced no documents that corroborate his testimony. *Id*. at 112:14-113:6; 115:6-22.

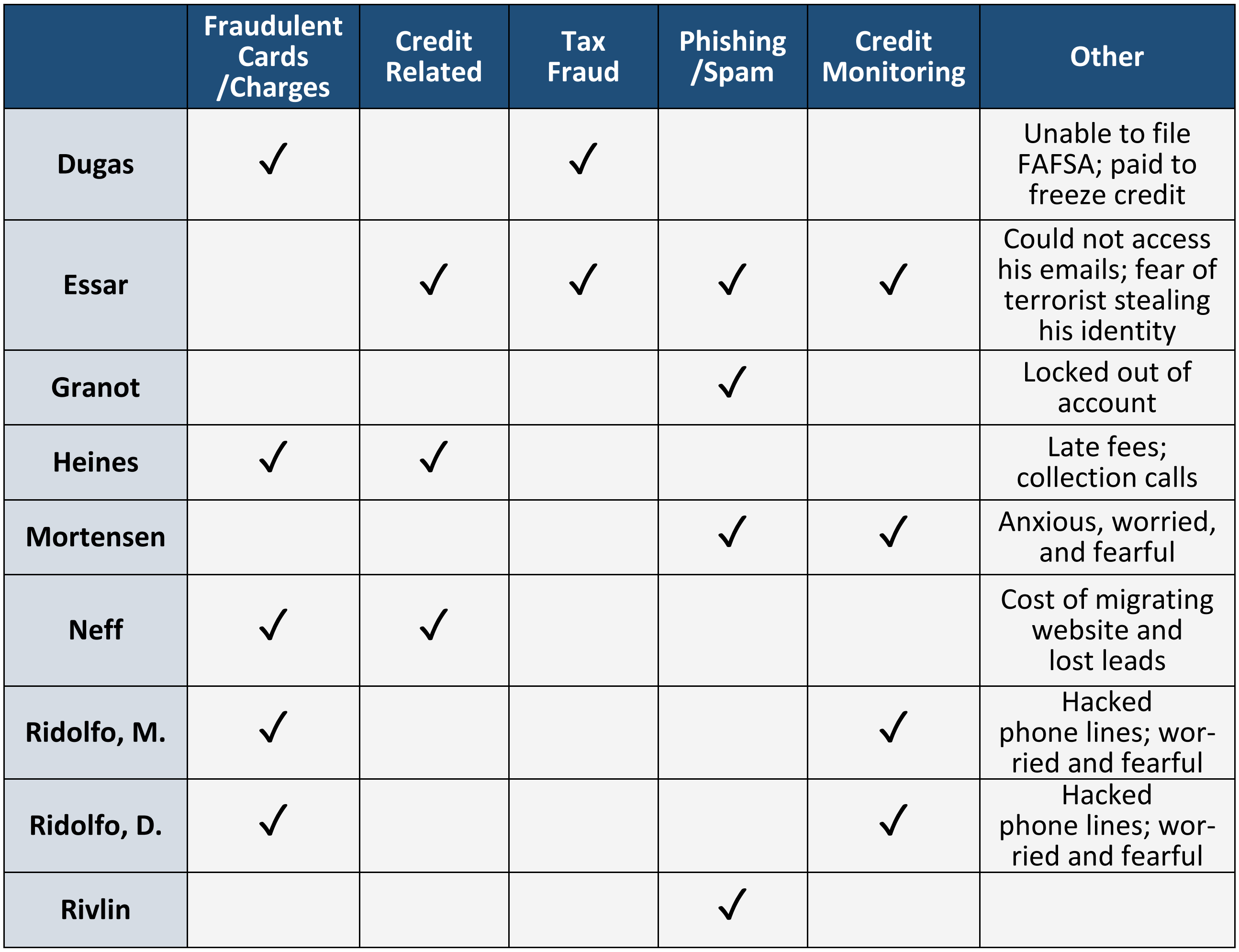
The amount of time, if any, that the email accounts were potentially accessible to criminals also varied by individual, depending on the individual user's responses to the attacks, and in particular, when he or she changed passwords. Ferrante Rpt. at 5-7. Those windows of opportunity could range from weeks to years. For example, Ms. Heines changed her password approximately two weeks after the date of the copy of the user database was stolen in the 2013 attack, whereas Mr. Dugas, to date, still may not have changed the password on one of his accounts. Whipple Decl. Exs. 20, 35. Mr. Essar did not change his password until approximately six months after the 2013 attack, but still did so before any Yahoo data was posted for sale on the dark web. *Id*., Ex. 28; Ferrante Rpt. at 6.

The evidence of actual intrusion by criminals varies by person, as well. For example, evidence shows that Russians infiltrated the accounts of Ms. Chalupa and other prominent persons of interest. *See* Tepstein Decl. Ex. 7 at 22; Ex. 88 ¶¶ 34, 36 [criminal indictment]; ECF 252-5 [SEALED]; Isikoff, *supra*, at 4. But there is no comparable evidence for the Named Plaintiffs' emails. Indeed, Mr. Neff admitted he has no evidence that his account was accessed by a criminal. Ex. 74 (Neff Dep.) at 161:10-25; 244:13-16. Mr. Neff and Mr. Essar both testified that the Yahoo accounts of their family members had not been affected in any way, including with respect to PII (i.e., addresses). Ex. 74 (Neff Dep.) at 266:4-267:20; Ex. 49 (Essar Dep.) at 26:22-25.

D. Alleged Injury and Connection to the Yahoo Attacks

Given the different practices and usage of Yahoo accounts by the Named Plaintiffs, their alleged experiences after the attacks are similarly varied, both in type and severity, as illustrated below:

Figure 1: Harms Alleged By Named Plaintiffs[3]



	Fraudulent Cards /Charges	Credit Related	Tax Fraud	Phishing /Spam	Credit Monitoring	Other
Dugas	✓		✓			Unable to file FAFSA; paid to freeze credit
Essar		✓	✓	✓	✓	Could not access his emails; fear of terrorist stealing his identity
Granot				✓		Locked out of account
Heines	✓	✓				Late fees; collection calls
Mortensen				✓	✓	Anxious, worried, and fearful
Neff	✓	✓				Cost of migrating website and lost leads
Ridolfo, M.	✓				✓	Hacked phone lines; worried and fearful
Ridolfo, D.	✓				✓	Hacked phone lines; worried and fearful
Rivlin				✓		

Whether these harms can be connected to Yahoo, much less found to have resulted from the attacks, also varies from user to user, as the Named Plaintiffs themselves acknowledge:

[3] ECF 196 ¶¶ 18-24, 26-28.

– Mr. Essar: "[S]ome people who use Yahoo mail may not have suffered any harm at all"— "*it's an individualized issue.*" Ex. 49 (Essar Dep.) at 230:8-13 (emphasis added).

– Ms. Granot: "Of course," "some people may have suffered more harm than others." Ex. 52 (Granot Dep.) at 244:23-245:1.

– Ms. Heines: "Well if your identity is stolen, you can – you know, you lose all your money, people do bad things with your – you know, they take people's stuff and they, you know, can ruin them. I mean there are varying degrees; right? I mean it could be simple, or it could be life devastating." "What is harm to one is not harm – you know, for me, losing $1,100 was a great harm." Ex. 55 (Heines Dep.) at 165:15-24.

– Mr. Mortensen: "The harm [from a data breach] is of course theoretical, potential." Ex. 60 (Mortensen Dep.) at 87:21-22. "It's hard to decipher which [type of personal information] is more important than the other"; "It's highly variable" "in different circumstances." *Id.* at 207:15-20.

– Ms. Ridolfo: "Certain people have been affected in different ways." Ex. 77 (Ridolfo Dep.) at 171:4-5. There are "different consequences for different people." *Id.* at 176:21-22. "[W]e are worst-case scenario." *Id.* at 170:13-14.

The evidence developed in discovery underscores that this is in fact the case. Take Ms. Heines's experience with debit card fraud. There, the fraudster made three charges on Ms. Heines's debit card, and the evidence shows the charges were made by swiping the magnetic stripe of a debit card—not online or over the phone. Ferrante Rpt. at 25. To do so, the fraudster must have made a fake physical card because Ms. Heines had her own card in her possession. Ex. 58 (Rog response No. 12). That requires the numbers from the magnetic stripe of the debit card, which the human eye cannot read. Thus, it could not possibly have been taken from the user database or from Ms. Heines's Yahoo email account. Ferrante Rpt. at 25-26. Instead, Ms. Heines's debit card was likely captured and cloned by a payment card "skimmer," which can copy the hidden numbers and thereby allow a criminal to make a fake card. *Id.*

Mr. Dugas alleges he was injured because someone allegedly filed fraudulent tax returns in his name, which caused him to incur penalties and to miss the deadline to submit student loan applications for his daughters. ECF 196 ¶ 20. But that, too, did not result from the attacks on Yahoo. Once placed under oath, Mr. Dugas conceded that the fraudulent 2013 and 2014 business tax returns were not caused by the attacks on Yahoo, but by the fact he was in the hospital. Ex. 37 (Dugas Dep.) at 256:24-257:4; 258:5-11; 259:5-260:15. The 2015 tax fraud he alleges also likely has no connection to the attacks, as

Mr. Dugas admitted that he only "assumed" there was a "causal relationship" between the 2015 fraudulent return and the attacks on Yahoo based on the timing and his "intuition." *Id*. at 33:6-13; *see also* 28:4-29:10. To commit tax fraud, however, a criminal would have needed Mr. Dugas's Social Security number, which Mr. Dugas "do[esn't] recall" sending through a Yahoo email account, and there is no evidence to suggest he ever did. *Id*. at 30:9-24; 116:19-21; Ferrante Rpt. at 29-30.

These are just two examples. Anthony Ferrante, the former Chief of Staff of the FBI's Cyber Division and Director for Cyber Incident Response at the U.S. National Security Council at the White House, has examined the evidence related to each of the Named Plaintiffs' alleged injuries using the techniques and methods he and others use in law enforcement. Ferrante Rpt. at 2-3, 23-58. His conclusions regarding the likelihood that those injuries were connected to, much less caused by, the attacks on Yahoo (in categories of "not caused," "very likely not caused," "possibly caused," or "very likely caused") are set forth in the Ferrante Report filed with this brief.

In sum, the evidence shows that the PII accessed, the harm caused, and the link to the attacks on Yahoo all varied substantially across users. Many users would have had no PII in their accounts. Where they did, what was accessed varied depending on what information the user provided to Yahoo, whether it was fake or stale, and the window of time during which the PII was available to cybercriminals. Some complain of spam and phishing emails while others allege tax fraud or an inability to file loan documents. And whether any of that was tied to the attacks depends on the alleged injury, and an infinite range of intervening causes.

E. The Paid User and Small Business Sub-Classes

Plaintiffs also have proposed sub-classes for those users who paid for Yahoo services, as well as those who used Yahoo for their small businesses. Andrew Mortensen, the putative representative for the paid user class, admitted that though his telephone number and zip code were accurate at the time he signed up and at the time of the 2013 attack, that information is now outdated. *See* Ex. 60 (Mortensen Dep.) at 10:9-11; 36:14-38:5; 108:24-110:23;116:19-117:11. He described his injury as "theoretical, potential" (*id*. at 87:21-22) and admitted he could not link it to Yahoo, nor quantify it (*id*. at 210:4). Indeed, despite purporting to represent the paid user class, he admitted that his decision to purchase a premium Yahoo account had nothing to do with security, and said he was not "seeking any financial compensation" from the suit. *Id.* at 113:12-114:15; 117:12-118:7; 124:14-125:16; 250:12-13. He further admitted that he has not taken any remedial measures recommend by Yahoo or otherwise in response to the attacks on Yahoo. *Id.* at 173:2-174:1.

Brian Neff, the putative representative for the small business class, who operated [redacted] [redacted]" using Yahoo's small business services, admitted that he [redacted] [redacted] Ex. 74 (Neff Dep.) at 9:23-10:13, 56:13-57:3. Unlike Mr. Mortensen, he alleged less "theoretical" injuries, including credit card fraud, costs incurred in migrating his business to another website, the loss of certain business leads, a lower credit score, and difficulty qualifying for a home mortgage (ECF 196 ¶¶ 26-27), but could not "assign a monetary value" to any of them (Ex. 74 (Neff Dep.) at 261:18-24). In addition, although his wife and daughter had Yahoo accounts through the small business service, neither has suffered any identity theft. *Id.* at 266:4-267:20. Further, he did not continue to use his business website, but instead shut it down immediately after being notified of the attack on Yahoo. *Id.* at 127:15-128:21. He disclaims any intention to use it in the future. *Id.* at 114:7-17. He further admitted that "every business is different" and that small business users would have "different uses" and "different forms" of websites. *Id.* at 278:8-14.

III. The Court Should Not Certify Any of Plaintiffs' Proposed Classes or Sub-Classes

Each of Plaintiffs' proposed classes fails to meet Rule 23's stringent requirements. Their Rule 23(b)(3) sub-classes fail because critical liability elements of their claims—injury and causation—cannot be established without individualized inquiries that will overwhelm any common questions. Their injunctive relief class fails because their proposed class representatives have not alleged that they will be immediately re-injured by Yahoo (*Chapman*, 631 F.3d at 946), much less offered "evidentiary proof" (*Comcast*, 569 U.S. at 33, 34). And their issue classes fail because the proposed issues cannot answer, or even narrow the answers to, the key questions of who was harmed or by how much, much less whether any harm is attributable to Yahoo.

A. The Free and California User Sub-Classes Cannot Meet the Rule 23 Prerequisites

Plaintiffs have failed to identify questions that "predominate" over the individualized inquiries necessary to resolve their claim elements, Yahoo's defenses, or to establish an entitlement to relief. Their failure to satisfy the "demanding" requirements of Rule 23(b)(3)—predominance, superiority, and manageability—is fatal to their proposed nationwide Free User and California User sub-classes. *Comcast*, 569 U.S. at 34. That is because *every* claim for which Plaintiffs have sought (b)(3) certification—the contract claims, negligence claim, and violation of the California Customer Records Act—requires them to prove *to the jury* that the class members were *harmed* and that Yahoo *caused* that harm. *See Erica P. John Fund, Inc. v. Halliburton Co.*, 563 U.S. 804, 809-10 (2011) (predominance inquiry "begins . . . with the elements of the underlying cause of action") (citations omitted); *Davidson*, 2018 WL 2325426, at *14 (explaining that the most "important[]" and "critical question" for certification under Rule 23(b)(3) is "whether common evidence and common methodology could be used to prove the *elements* of the underlying cause of action").

Plaintiffs argue that "each of the claims [they] seek to advance turn on the question of whether Defendants' security protocols and policies were adequate to protect Class members' PII." Mot. at 14; *see also id.* at 15 ("the inadequacy of Yahoo's security protocols and procedures also resulted in the same fundamental injury to each Damages Class member"). And they flag a number of additional issues that they contend are "common to Damages Class members," including "whether Defendants breached the TOS by failing to adequately safeguard PII." *Id.* at 14. Curiously absent, however, are other equally and admittedly essential elements of their negligence and breach of contract claims, namely, harm and causation. *See* Mot. at 22, 24; *see also* CACI 303 (plaintiff "must prove" that he or she "was harmed" and that the "breach of contract was a substantial factor in causing [his or her] harm"); CACI 400 (plaintiff "must prove" he or she "was harmed" and that the "negligence was a substantial factor in causing [his or her] harm"). The same is true of the Customer Records Act—*i.e.*, Plaintiffs must prove it is more likely than not that each absent class member suffered "actual damages flowing from the unreasonable delay (and not just the intrusion itself)." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014), *order corrected*, 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014); *see also* Cal. Civ. Code § 1798.84 ("Any customer *injured by a violation* of this title may institute a civil action to recover damages." (emphasis added)).

Plaintiffs erroneously and improperly attempt to recast these threshold questions of liability as whether "damages may ultimately require individual calculation." Mot. at 27. But the elements of *liability* demonstrate the fallacy of that argument. The correct question is "whether common evidence and common methodology could be used to prove the *elements* of the underlying cause of action." *Davidson*, 2018 WL 2325426, at *14 (emphasis added); *see also Senne v. Kansas City Royals Baseball Corp.*, 315 F.R.D. 523, 578 (N.D. Cal. 2016), *appeal pending* (explaining that variations in the types of activities class members performed are "individualized issues that go not only to damages but also to liability"). The answer to that dispositive question is undeniably "no," inasmuch as no classwide evidence establishes that "common PII" was exposed in the attacks (Mot. at 30-31, 35), or that any of the allegedly resultant harms were caused by Yahoo. Again, the evidence for two Named Plaintiffs is instructive: Plaintiff Heines alleges she experienced debit card fraud and claims Yahoo is at fault for it. ECF 196 ¶ 18. But discovery has shown that the information needed to commit the debit card fraud was *not* in Yahoo's user database or her email, and thus her harm was not caused by Yahoo. *See* Ferrante Rpt. at 25-26. In contrast, Plaintiff Matthew Ridolfo alleges his identity was stolen and used to fraudulently open multiple credit card and bank accounts, and he testified that the necessary information to commit identity fraud *was* in his Yahoo email. *Id.* at 34; Ex. 80 at 53:1-54-8. Those dissimilarities—when considered across millions of putative class members—are fatal to Plaintiffs' claims.

Plaintiffs attempt to paper over the individual variations across the class members with their "Lost Value of PII" and the "Identity Theft Losses" models. The first model promises to use "statistical sampling to determine the PII in an average users' account and the value of that PII." Mot. at 27, 29. The second model promises to show how class members should be compensated for "identity theft losses" by proving in the abstract that the attacks caused the putative class members to suffer an "increased risk of future harm." *Id.* at 30. Plaintiffs propose that a claims or other administrator then award relief for specific "identity theft losses," provided the alleged injury occurred after one of the attacks (a "temporal connection"). *Id.*

Rather than demonstrate that common questions predominate, these proposals lay bare the absence of common proof here. The "Lost Value of PII" model assumes that the PII provided by class members in fact had value—i.e., that it was true, up-to-date, and not freely available elsewhere, but the evidence shows that assumption is false. The "Identity Theft Losses" model assumes that harms from identity theft can somehow be standardized or else managed through a claims process. But the evidence disproves the former, and the Seventh Amendment bars the latter.

1. Whether Class Members "Lost Value" in Their PII Will Require Numerous and Unmanageable Individual Inquiries

Because users had significant freedom to decide what information to enter into Yahoo's user database and often did not enter truthful information, because even the true information grew stale over time, and because some of the information was also publicly available, there is no way to determine on a classwide basis what PII (if any) was exposed for any individual user, much less determine for all users whether Yahoo can be held accountable for any diminution in value for the PII. Instead, discovery has shown that at least three distinct individual inquiries will be required to determine whether a given putative class member lost value in his or her PII because of the attacks on Yahoo.

Plaintiffs contend that "expert testimony" can establish, among other things, that "all members of the Damages Class suffered the lost value of their PII and an increased risk of future harm" and that "there is a logical and foreseeable causal connection between Defendants' failures and these injuries." Mot. at 26-27. But these contentions will not make "issues going to [harm and] causation . . . minimal." *Id*. at 27. Plaintiffs' Rule 23(b)(3) sub-classes accordingly cannot be certified under this theory.

Whether Plaintiffs Provided or Transmitted Any PII to or Through Yahoo. Plaintiffs are wrong in their assertion that a "common" set of PII exists across the class. Mot. at 30; ECF 258-4, Ex. 94 [Van Dyke] ¶ 30 (assuming 100% of putative class members entered a real name, address, telephone number, and birthdate into Yahoo's user database). Yet this is a critical liability inquiry: Yahoo cannot be held responsible for a diminution in value if the PII was fake to begin with.

There are likely millions of putative class members who fit into this "no PII" bucket and thus "could not have been injured by Defendant's alleged wrongful conduct." *Moore*, 309 F.R.D. at 542-43. [redacted] *E.g.*, ECF 254-10 [Ratner Rpt.] ¶ 10 [SEALED]; Ex. 84 (Rivlin Dep.) at 40:1-24 (noting he may have opened a "dummy" account); Chhabra Decl. ¶ 12; Ex. 99 (Ratner Dep). at 137:7-20 (acknowledging that dummy accounts will not have PII associated with them). A review of aggregate data from the 2016 user database (the most readily accessible database with user information) shows, for example, that:

- Over [redacted] million accounts had no name; over [redacted] use a single punctuation mark as a last name, over [redacted] use “John Doe,” [redacted] use “Bruce Wayne,” and [redacted] use “[redacted]
- Almost [redacted] accounts had no phone number listed.
- Over [redacted] accounts supposedly had owners over the age of 122, and over [redacted] account holders just happen to be turning 118 years old this year.
- Over [redacted] accounts supposedly had owners born on [redacted] which is more than six times as many as the next most common birthday, February 2.
- Over [redacted] accounts had the zip code 12345—the zip code a General Electric’ plant that has *no* population. Another [redacted] accounts use the zip code 90210, made famous by the television show “Beverly Hills 90210,” even though that zip code has only 35,000 residents.

See Whipple Decl. ¶¶ 12-15, 18; *id.*, Exs. 11-14; Tucker Rpt. ¶¶ 87-91.

To determine whether “Luke Skywalker” is the true name of the child of two Star Wars fanatics, and if so, whether he is in the class—will require individual inquiries. That is true writ large: because *all* of the PII at issue here was entered by users, the only way to know whether it is real is an account-by-account or user-by-user inquiry. *See* Whipple Decl. ¶¶ 4-5; *id.*, Ex. 10 (2012 UDB data for Granot showing fake entries). Nor was there any “common” or “average” amount of PII, as an examination of the telephone numbers, birthdates, and zipcodes provided by the Named Plaintiffs exemplifies:[4]

[4] Checks indicate that the information provided was true and current. Null sets indicate that no information was provided for this particular category of PII. Multiple entries within a particular cell indicate that the user had multiple accounts.

This chart reflects the data each Named Plaintiff likely inputted to Yahoo’s user database when signing up for Yahoo or at some point thereafter. Because some Named Plaintiffs were affected by the 2013 attack, and others by the 2014 attack, the chart lists the data as “stale” if it was already outdated at the time of the relevant attack. The telephone numbers and zip codes evaluated are those that were entered by the users in the personal information fields (not in the business or alternate communication channels fields). Whipple Decl. Ex. 10; Ex. 37 (Dugas Dep.) at 12:16-19, 13:14-15, 84:12-14, 85:1-24, 87:6-10, 88:1-3, 88:7-9; Ex. 49 (Essar Dep.) at 8:6-7, 32:14-18, 37:15-38:9; Ex. 52 (Granot Dep.) at 9:6-8, 7:23-8:13; Ex. 55 (Heines Dep.) at 11:6-7, 34:16-36:19, 88:11-18; Ex. 60 (Mortenson Dep.) at 11:5-8, 36:14-38:5, 108:24-110:20; Ex. 74 (Neff Dep.) at 8:8-12, 9:23-10:13, 53:2-7, 56:13-57; Ex. 80 (M. Ridolfo Dep.) at 7:10-8:2, 8:10-11; Ex. 77 (D. Ridolfo Dep.) at 7:10-16, 7:19-8:5; Ex. 84 (Rivlin Dep.) at 10:9-11.

Figure 2: Status of Selected User Database Information for Named Plaintiffs

	Telephone Number	Birthdate	Zip Code
Dugas	Fake & Ø & Fake	Fake & ✓ & Fake	Fake & Stale Work Zip Code & Fake
Essar	Ø	Fake	Work Zip Code
Granot	Ø & Ø	✓ & Fake	Fake[5] & Fake
Heines	Stale	✓	Stale
Mortensen	✓ & Ø	✓ & ✓	✓ & ✓
Neff	Wife's #	✓	Stale
Ridolfo, M.	Ø	✓	✓
Ridolfo, D.	✓	Husband's	Fake
Rivlin	Ø	✓	Ø

Plaintiffs' Lost Value of PII model, however, is not limited to the few categories of information stored in Yahoo's user database. Plaintiffs seek to recover for the lost value of PII contained in each class member's *emails* too, which critically, are not stored in Yahoo's user database. Mot. at 28. But this only introduces "an additional link in the 'causal chain," and thus more material differences from class member to class member. ECF 132 at 31 (granting in part Yahoo's first motion to dismiss). Now, to determine whether any given user was harmed, the jury will need to examine whether the class member had an email account, whether they ever sent PII using that account, and whether anyone "*then* accessed the sensitive personal information contained within Plaintiffs' email accounts." ECF 132 at 31 (emphasis in original). Here, too, the Named Plaintiffs' testimony and produced documents confirm these issues cannot be resolved on a classwide basis. Take, for example, the question whether the Named Plaintiffs transmitted Social Security numbers or full payment card numbers through their Yahoo emails:

[5] Ms. Granot listed the zip code [redacted] when signing up for her [redacted] account. Whipple Decl. Ex. 10. If this is an [redacted] zip code, it does not appear to correspond to [redacted] where she has lived since 2003 (with the exception of one year when she was studying at Harvard). Ex. 52 (Granot Dep.) at 7:23-8:13. If this is a United States zip code, it corresponds to [redacted] where she has never lived. *Id.*

Figure 3: Transmission of SSN and Full Payment Card Numbers by the Named Plaintiffs[6]

	Social Security #	Payment Card #	Evidence in Support
Dugas	Ø	Ø	Ø
Essar	✓	Ø	**Testimony**
Granot	Ø	Ø	Ø
Heines	✓	✓	**Document for SSN; Ambiguous testimony for Payment Card #**
Mortensen	✓	✓	**Documents**
Neff	✓	✓	**Documents**
Ridolfo, M.	✓	Ø	**Testimony**
Ridolfo, D.	Ø	Ø	Ø
Rivlin	Ø	✓	**Documents**

As this chart shows, only three of the nine Named Plaintiffs shared both their Social Security number and a full payment card number, and only two have documents to prove it. Where even a generous assessment shows fewer than 50% of the Named Plaintiffs experienced the claimed injury, there can be no credible suggestion of common classwide harm, and there is no way to avoid compensating uninjured class members who cannot recover under the substantive law and have no right to bring a claim in federal court. *See Comcast*, 569 U.S. at 35 (explaining that a "plaintiff's damages case must be consistent with its liability case"); *Tyson Foods, Inc. v. Bouaphakeo*, 136 S. Ct. 1036, 1053 (2016) (Roberts, C.J., concurring) (explaining that a class action judgment should reward "only . . . injured class members"); *see also Moore*, 309 F.R.D. at 542-43 (rejecting a proposed class for lack of predominance because "it necessarily includes individuals who could not have been injured by Defendant's alleged wrongful conduct as a matter of law").

The Value of the PII Before the Attacks. The value of a given class member's PII is equally critical for determining liability. If a class member stored PII with Yahoo, but it is worthless, then the

[6] Ex. 49 (Essar Dep.) at 72:3-73:4; Ex. 55 (Heines Dep.) at 135:5-137:13, 153:20-154:13, 204:5-205:12; Ex. 80 (M. Ridolfo Dep.) at 221:3-222:15; Ex. 56 (Heines000608-610); Ex. 71 (AMORTENSEN000094-96); Ex. 70 (AMORTENSEN002442-43); Ex. 85 (Rivlin005724-26); Ex. 75 (Neff001426-45).

class member cannot recover any "loss" in value, much less claim that the loss was caused by Yahoo. As the Named Plaintiffs themselves again demonstrate, this is another intractably individualized issue. Mr. Dugas, for example, provided Yahoo with mostly fake information, or information that was outdated by the time of the attacks on Yahoo, and thus there would be little reason for anyone to pay for it. Ex. 37 (Dugas Dep.) at 12:16-19, 13:14-15, 84:12-14, 85:1-24, 87:6-10, 88:1-3, 88:7-9; Whipple Decl. Ex. 10. Indeed, Mr. Dugas's old business address and current phone number were listed on a public website, associated with his business, and easily accessible via Google, until after his deposition. Ex. 37 (Dugas Dep.) at 127:15-129-7 & Ex. 4. Mr. Mortensen did provide his telephone number to Yahoo, but testified that he had voluntarily provided that number to more than 20 companies. Ex. 60 (Mortensen Dep.) at 242:22-243:1. Mr. Ridolfo, by contrast, did provide an accurate and up-to-date address and birthdate. Ex. 80 (M. Ridolfo Dep.) at 7:10-16, 8:10-11; Whipple Decl. Ex. 10. A fraudster would value Mr. Ridolfo's more accurate and current more highly than Mr. Dugas's or Mr. Mortensen's fake or outdated information, but Plaintiffs' proposals would assign all the same value, thereby multiplying the value of the claims here, in violation of Yahoo's due process rights (*Dukes*, 569 U.S. at 367) or else (in the absence of a waiver of Yahoo's Seventh Amendment rights), generating conflicts among members of the class by overcompensating some while undercompensating others (*see Standard Fire Ins. Co. v. Knowles*, 568 U.S. 588, 593-94 (2013)).[7]

Whether Any Decrease in Value Was Caused by the Attacks. Once the jury has decided whether a particular user stored any PII with Yahoo and determined a baseline value (if any) of that PII for the period before the attacks on Yahoo, the jury will still have to determine (1) whether the value of the PII has decreased since the attacks *and* (2) whether that decrease was caused by Yahoo.

As even Plaintiffs' experts admit, there are myriad reasons, unrelated to Yahoo, why the value of the PII in Yahoo's user database might fluctuate, such as the person's own practices of publicizing

[7] The Court should not conflate, as Plaintiffs' experts have (*see* Ex. 99 (Ratner Dep.) 163:12-20), the concept of lost value of PII with the concept of increased risk of identity theft. The lost value of PII concept is an inherently comparative model of damages: Had Yahoo protected Plaintiffs' PII, it would have been worth so much; because it allegedly did not, it is now worth less. The measure of damages is the difference between those two values. An increased risk of identity theft might be relevant to the second value (i.e., the PII is worth less not just because others have it, but because they could potentially cause further harms with it), but it is not equivalent to the delta between the value of PII before and after the breach. *See, e.g.*, Ex. 99 (Ratner Dep.) at 255:8-256:10 (differentiating between the diminution in value and risk of loss as two separate measures of damages).

their PII, or whether the person is a "high-value target[]." ECF 252-17 [Frantz Report] at 7 [SEALED].. Further, while the cybercriminals gained access to Yahoo's user database and could view the telephone numbers, birthdays, and some zip codes for many putative class members (ECF 250-10 [Yanchunis Decl., Ex. 29] at YMDL008625972), their access to putative class member emails was more limited, and generally targeted specific persons of interest. Thus, proving that a person's PII lost value because cybercriminals accessed their *email*—not just the information in the Yahoo database—will require even more individual inquiries. Indeed, *none* of the Named Plaintiffs presented evidence that cybercriminals had actually accessed their stored Yahoo emails. To the contrary, Mr. Neff candidly admitted he had no evidence that any unauthorized person accessed his emails (Ex. 74 (Neff Dep.) at 161:10-25; 244:13-16) and admitted, along with Mr. Essar, that the accounts of his family members were unaffected. *Id.* at 266:4-267:20; Ex. 49 (Essar Dep.) at 26:22-25. By contrast, because the hackers targeted Alexandra Chalupa and other prominent individuals, those individuals would have evidence to present to the jury. Isikoff, *supra,* at 4. These individual variations amply demonstrate why this case, if certified, will rapidly "'degenerat[e] into a series of individual trials.'" *Moore*, 309 F.R.D. at 549 (quoting *Gene & Gene LLC v. BioPay LLC*, 541 F.3d 318, 326 (5th Cir. 2008)); *see also Smith v. U.S. Bank, N*.A., 2017 WL 698530, at *10 (S.D. Fla. Feb. 22, 2017) (declining to certify contract claims where causation and harm would require individualized proof).

2. Plaintiffs' Experts Cannot Make the Individual Inquiries Disappear

Plaintiffs gloss over these three individual inquiries, contending that they can establish injury and causation by "surveying consumers as to the type of PII they have emailed" and then using "a market-based approach to determine Class members' damages resulting from the diminution of value of their PII as a result of the Data Breaches." Mot. at 29. Neither proposal is admissible. *See* Motions to Exclude Plaintiffs Experts, filed concurrently with this motion. But even if they were, they are not a valid basis upon which to certify a class.

First, the proposal to use the results of a survey—designed to represent the U.S. population, *not* the population of Yahoo users (ECF 258-4, Ex. 94 [Van Dyke] at Ex. A, p. 27)—to determine that each absent class member had an "average of 11.5 listed identity records" (*id.* ¶ 35), is the kind of "'Trial By Formula'" the Supreme Court rejected in *Dukes*, 564 U.S. at 367, and *Tyson Foods*, 136 S. Ct. at

1049, and has otherwise been rejected in the Northern District. *See, e.g.*, *Senne*, 315 F.R.D. at 583 (rejecting attempt to "paper over significant material variations that make application of the survey results to the class as a whole improper"); *In re Autozone, Inc*., 2016 WL 4208200, at *15 (N.D. Cal. Aug. 10, 2016) (rejecting use of a survey about employees' rest breaks because the same evidence could not be used in an individual action to establish liability). A "representative sample may be used to establish classwide liability" only if "the sample at issue could have been used to establish liability in an individual action." *Tyson Foods*, 136 S. Ct. at 1049. The survey in *Tyson Foods* satisfied that rule because the employee-plaintiffs were "similarly situated"—"each employee worked in the same facility, did similar work, and was paid under the same policy"—and there were no records of the time any employees spent "donning and doffing." *Id.* at 1044, 1048. Because each employee would have to rely on the survey to prove an individual claim, the Court saw no difficulty with allowing the class to rely on the survey to prove the class claims. *Id.* at 1048.

That sort of proof does not exist here. If Mr. Dugas, for example, were to pursue his case on an individual basis, he could not (and would have no reason to) introduce evidence that email users send or receive an "average of 11.5 listed identity records," because he has his *own* evidence of how much PII he gave to Yahoo and stored in his email, and that evidence shows that putative class members are not similarly situated. *See* Whipple Decl. Ex. 10. How much PII an "average" accountholder stored in her email would be entirely irrelevant (and thus inadmissible) and could not "sustain a jury finding" as to Mr. Dugas. *Tyson Foods*, 136 S. Ct. at 1049. Indeed, one of Plaintiffs' experts conceded that he would "never assume that any entity's customer base or user base is necessarily representative of the average U.S. person." Ex. 96 (Van Dyke Dep.) 195:14-25. Because a survey opining on what some invented "average" email user (and not even an average *Yahoo* user) had in his or her email account would not be admissible in an individual trial for any of the Named Plaintiffs—and would in many cases contradict the Named Plaintiffs' own testimony about their experiences—Plaintiffs cannot use it to manufacture a common issue without "violat[ing] the Rules Enabling Act by giving plaintiffs and defendants different rights in a class proceeding than they could have asserted in an individual action." *Id*. at 1048; *see also In re Hotel Tel. Charges*, 500 F.2d 86, 90 (9th Cir. 1974) (rejecting damages model that calculated only "average" injury as violating due process and the Rules Enabling Act).

Second, Plaintiffs' proposal to use a "market-based approach to determine Class members' damages resulting from the *diminution of value* of their PII as a result of the Data Breaches" (Mot. at 29, emphasis added) fails for a more fundamental reason: their experts, Ratner and Van Dyke, propose to (but do not actually) measure the "*total* expected value of the exposed personal information"—not the *loss* in value, *even though that is their theory of liability*. ECF 258-4, Ex. 94 [Van Dyke Rpt.] ¶ 77 (emphasis added); ECF 254-10 [Ratner Rpt.] at 9 ("Estimating the Value of PII"). Without attempting to "isolat[e] the damages attributable to Defendant's alleged wrongdoing," Plaintiffs have failed one of the key requirements for certification. *Werdebaugh*, 2014 WL 7148923, at *11 (citing *Comcast*, 569 U.S. at 35 (damages model "must measure only those damages attributable to [plaintiffs'] theory [of harm]")); *see also Bruton v. Gerber Prod. Co.*, 2018 WL 1009257, at *12 (N.D. Cal. Feb. 13, 2018) (rejecting a damages model where the expert "identified a number of variables that might prevent the proposed Regression Model from complying with *Comcast*'s requirements, but has failed to provide a meaningful explanation as to how the variables will be addressed"); *In re Rail Freight Fuel Surcharge Antitrust Litig.*, 725 F.3d 244, 254 (D.C. Cir. 2013) ("It is not enough to submit a questionable [damages] model whose unsubstantiated claims cannot be refuted through *a priori* analysis.").

Plaintiffs cannot camouflage this glaring flaw by arguing the "total expected value of the exposed personal information" is the same as the "loss in value" because the PII of class members became worthless after the attacks on Yahoo. Their experts' reports "never even state[]" "let alone justif[y] the conclusion that this assumption is correct" (*Philips v. Ford Motor Co.*, 2016 WL 7428810, at *21 (N.D. Cal. Dec. 22, 2016)), and there is no factual basis for such an assumption. Tucker Rpt. ¶ 130, 222. That alone is enough to reject the model and conclude that the proposed class "does not meet Rule 23(b)(3)'s predominance requirement," as this Court recognized in *Philips*. *See* 2016 WL 7428810, at *21 (rejecting a damages model that assumed the product's value plummeted to zero). The problem is even more acute here because if the value of a person's PII plummets to zero after a data breach—any data breach—then the individual inquiries regarding causation will grow exponentially. At the class certification stage, in which "evidentiary proof" and not just pleadings may be considered (*Comcast*, 569 U.S. at 33), Plaintiffs or class members whose data had been stolen previously would be barred from claiming any loss at all from the attacks on Yahoo (*see, e.g.*, Ferrante Rpt. at 18-22 [identifying earlier data breaches that affected Mr. Dugas]), and the factfinder would have to parse which data for each given user had been exposed in earlier breaches to determine who can recover and who cannot. That is the very opposite of classwide evidence.

3. Determining "Identity Theft" Losses Requires Unmanageable Individual Inquiries

In addition to their "Lost Value of PII" theory, Plaintiffs contend they can litigate this case by offering proof that putative class members suffered "identity theft losses." But identity theft, "by its very nature[,] [is] a highly personalized crime" with individualized causes (*Dolmage v. Combined Ins. Co. of Am.*, 2017 WL 1754772, at *7 (N.D. Ill. May 3, 2017)), and does not typically lend itself to classwide proof. Plaintiffs cannot rectify this problem through a claims process or by improperly shifting the burden of proving causation onto Yahoo.

To determine whether a putative class member suffered *harm* in the form of identity theft *because of* the attacks on Yahoo, the jury will have to conduct at least two individualized inquiries: (1) whether a given class member suffered any identity theft and if so, what kind, and (2) whether that identify theft was caused by the attacks on Yahoo. *See* CACI 303; CACI 400; Cal. Civ. Code § 1798.84. The facts surrounding the Named Plaintiffs' experiences demonstrate how quickly their claims of identity theft "'degenerat[e] into a series of individual trials.'" *Moore*, 309 F.R.D. at 549. As explained, Ms. Heines's alleged debit card fraud was not caused by the attacks on Yahoo—instead, the crime was committed using a fake card, and the information needed to make a fraudulent duplicate card was not stored by Yahoo. Ferrante Rpt. at 25-26. The same is true for Plaintiff Dugas, whose tax-fraud related harms were almost certainly not caused by Yahoo. ECF 196 ¶ 20; Ex. 37 (Dugas Dep.) at 30:9-24, 116:19-21; 282:25-283:10; Ex. 46; Ferrante Rpt. at 29-30.

Compare those Plaintiffs to Mr. and Ms. Ridolfo, who both allege that "a total of eleven credit card or bank accounts had been fraudulently opened" and that they lost "significant time" rectifying the situation (ECF 196 ¶¶ 21-22) because of the attacks on Yahoo. Unlike Ms. Heines and Mr. Dugas, Mr. and Ms. Ridolfo have [redacted] Ex. 77 (D. Ridolfo Dep.) at 153:17-154:21; Ex. 90 (confiscated journal). But there is no evidence that the parolee opened the fraudulent accounts or got the subject information *from Yahoo*. Thus, even with the journal, it is speculative to conclude the attacks on Yahoo caused the harm to Mr. and Ms. Ridolfo. Ferrante Rpt. at 37. And, of course, there is no suggestion the parolee's journal constitutes classwide proof.

"[C]ourts generally consider negligence claims ill-suited for class action litigation" for this exact reason: individual considerations predominate "[b]ecause the proximate causation analysis involves individualized factual issues." *Gartin v. S & M NuTec LLC*, 245 F.R.D. 429, 439 (C.D. Cal. 2007); *see also Smith*, 2017 WL 698530, at *10 (declining to certify class based on similar individualized issues for breach-of-contract claims). As one court recently said in denying class certification in a data breach case, "some" putative class members may have been an "actual victim of an actual theft of funds," but others will have suffered "no distress or inconvenience whatsoever" and are not entitled to any recovery. *Dolmage*, 2017 WL 1754772, at *7. Plaintiffs' experts confirmed as much: Ian Ratner admitted that "every account that's stolen or hacked or sold is not necessarily going to result in any downstream consequential damages to the owner of the account." Ex. 99 (Ratner Dep.) 149:3-18. And Mr. Van Dyke testified that one's vulnerability to identity theft—and the dollar cost thereof—would vary depending on, among other things, one's wealth and credit rating. Ex. 96 (Van Dyke Dep.) 243:8-246:1; *see also* Ex. 95 (Frantz Dep.) 144:6-147:2 (admitting that risk of identity theft depends on the individual). Determining who was harmed by the attacks on Yahoo will require individual inquiries. *See Dolmage*, 2017 WL 1754772, at *7-8.

4. These Individual Inquiries Cannot Be Managed or Minimized.

To attempt to avoid these necessarily individualized inquiries, Plaintiffs (1) seek to punt the necessary causation and harm analysis to "a basic claims process"; (2) use "statistical evidence . . . to determine the aggregate damages relating to identity theft by calculating the average user's out of pocket costs and required hours for identity fraud"; (3) argue that "it is Defendants' burden to disprove causation" because "the length of time between the Breaches and their notice has eviscerated much, if not all, of the evidence Defendants will claim is needed to show individual causation for every Damages Class member"; and (4) point to a single data breach case that has not been tried to judgment—*Smith v. Triad of Alabama, LLC*, 2017 WL 1044692 (M.D. Ala. Mar. 17, 2017)—as evidence that the "instances" of individual inquiries "are likely to be isolated and few." Mot. at 30-31. The law and the facts refute all four contentions.

First, harm and causation cannot be resolved through "a basic claims process," just as they cannot be resolved through thousands or millions of mini-trials before this Court. Mot. at 30. Not only would such a process require potentially millions of mini-trials, it would infringe on Yahoo's constitutional rights. As Plaintiffs concede, it is black-letter law that the *jury* must determine causation and harm. *Id*. at 30 (emphasis added); *see also* CACI 303; CACI 400; *In re iPhone Application Litig.*, 2011 WL 4403963, at *9 (N.D. Cal. Sept. 20, 2011) (quoting *Aas v. Super. Ct.*, 24 Cal. 4th 627, 646 (2000)) (explaining that an "appreciable, nonspeculative, present injury" is "an essential element of a tort cause of action"). Delegating that role to a non-judicial claims administrator would strip Yahoo of its Seventh Amendment right to a jury trial. *See Dukes*, 564 U.S. at 345, 367 ("[A] class cannot be certified on the premise that [the defendant] will not be entitled to litigate its statutory defenses to individual claims."); *Gallick v. Baltimore & O. R. Co.*, 372 U.S. 108, 115 (1963) ("It is the jury. . . which is the fact-finding body. . . . whether it relates to negligence, causation or any other factual matter.").

Moreover, Plaintiffs' proposal would be unworkable in practice. Plaintiffs propose to prove that the attacks "increased [class members'] risk of future harm," and then let the administrator award relief for specific "identity theft losses" so long as class members can prove any injury occurred after one of the attacks. Mot. at 30. According to Plaintiffs, this would "establish both a temporal and a logical connection between the Breaches and Damages Class members' injuries." *Id.* Discovery, however, has revealed the falsity of these assumptions. For example, although Ms. Heines's debit card fraud occurred after two of the attacks, the evidence shows that the attacks on Yahoo had nothing to do with causing that harm. Ferrante Rpt. at 25-26. Mr. Dugas's tax fraud also occurred after the attacks on Yahoo, but it likely had nothing to do with Yahoo because his Social Security number was *not* in his emails. Ex. 37 (Dugas Dep.) at 30:9-24; 116:19-21; Ferrante Rpt. at 29-32. There is simply no substitute for conducting discovery and examining the actual evidence on a harm-by-harm, person-by-person basis. But that could consume decades. Plaintiffs have stated that some of the sub-classes contain "millions of users." Mot. at 32. If even 10% of those users submitted claims, and if each of those users had to testify for an hour in support of their claims and the administrator needed 30 minutes to assess the relevant documents, a claims administrator would have to work ten hours a day, 365 days a year, for more than 40 years just to get through those claims. And to the extent Plaintiffs' theory of liability assumes that *everyone* would submit a claim, the process could add up to 405 years.

Second, Plaintiffs cannot use "statistical evidence" of an "average user's out-of-pocket costs and required hours for identity fraud" to "paper over" the evidence showing *actual* harms vary enormously and that many class members suffered no harm. *Senne*, 315 F.R.D. at 581, 583; *supra* at 7-9. Plaintiffs cannot wrap the "Trial by Formula" wolf in sheep's clothing to create the appearance of predominance. *Dukes*, 564 U.S. at 367; *Tyson Foods*, 136 S. Ct. at 1048. And for good reason. Consider Named Plaintiff Heines, who testified that she suffered from debit card fraud, that it caused her to lose over a thousand dollars due to the "cascade effect" on her finances and her financial situation, and that she spent 40 hours resolving the issue. Ex. 55 (Heines Dep.) at 242:24-247:8; Ex. 58 (Rog response No. 12). Rather than suggest that Ms. Heines' experience meaningfully reflects other members of the class, Plaintiffs implicitly concede it does not, offering instead to use an "average" person's loss in "generic incidents." ECF 258-4, Ex. 94 [Van Dyke] ¶ 50. That the actual evidence was not deemed typical of others underscores the absence of any "average" experience here.

Perhaps recognizing this problem, Plaintiffs have not even provided the Court with these supposedly reliable "averages" or even the "data" they plan to use to create them. ECF 258-4, Ex. 94 [Van Dyke] ¶ 50. That falls far short of establishing "common evidence and common methodology [that] could be used to prove the ***elements*** of the underlying cause of action." *Davidson*, 2018 WL 2325426, at *14 (emphasis added); *Dolmage*, 2017 WL 1754772, at *7 (distinguishing between calculating damages and proving a breach of contract claim). The most pressing question here is which class members were "injured by Defendant's alleged wrongful conduct" *at all*, not merely by how much. *Moore*, 309 F.R.D. at 542-43. By stating only that "it is *possible* to calculate" an "average victim's out of pocket costs and required resolution hours" (ECF 258-4, Ex. 94 [Van Dyke] ¶ 50), Plaintiffs cannot show predominance "'through evidentiary proof.'" *Moore*, 309 F.R.D. at 538 (quoting *Comcast*, 569 U.S. at 35); *Philips*, 2016 WL 7428810, at *21; *In re ConAgra Foods, Inc.*, 302 F.R.D. 537, 577 (C.D. Cal. 2014).

Third, Plaintiffs' attempt to shift the burden of proof to Yahoo is not only irrelevant for purposes of class certification but flatly wrong. Where the burden rests makes no difference for class certification because Yahoo has a constitutional right to "litigate its … defenses to individual claims." *Dukes*, 564 U.S. at 367. Affirmative defenses can, and often do, "overwhelm any common issues." *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *21 (N.D. Cal. Mar. 18, 2014); *Johnson v. Yahoo! Inc.*, 2018 WL 835339, at *2-3 (N.D. Ill. Feb. 13, 2018) (explaining "affirmative defenses can predominate such that a class should be decertified" and then decertifying the class because the "evidence" became "sufficient to justify an individual consent inquiry for a significant percentage of the class"); *Gene*, 541 F.3d at 327 ("[T]he predominance of individual issues necessary to decide an affirmative defense may preclude class certification.").

In any event, as CACI 303 and CACI 400 make clear, the burden of proof *does* fall squarely on Plaintiffs. In response, Plaintiffs cite *Haft v. Lone Palm Hotel*, 3 Cal. 3d 756 (1970), in which the California Supreme Court held that the defendant hotel had to prove that not providing a lifeguard did not cause the plaintiff's drowning because "the precise injury that the statutory provision [at issue] was intended to prevent" was drowning, and "the absence of definite evidence on causation is a direct and foreseeable result of the defendants' negligent failure to provide a lifeguard." *Id.* at 773. Neither is true here. Identity theft is not the "precise injury" that the actions for negligence and breach-of-contract were created to prevent centuries ago. And there is no lack-of-causation evidence, much less a lack of causation evidence due to any negligence by Yahoo. The necessary evidence is available, as the discussion above demonstrates with respect to Ms. Heines, Mr. Dugas, Mr. Ridolfo, and Ms. Ridolfo—it is simply individualized and incapable of being extrapolated across the class. Indeed, Mr. Ferrante has examined extensive evidence for every Named Plaintiff, just like the jury would need to do to draw conclusions about harm and causation. *See* Ferrante Rpt. at 23-58. That Plaintiffs would prefer to ignore the actual evidence and its individualized nature is not a reason to shift the burden of proof to Yahoo. *See Thomas v. Lusk*, 27 Cal. App. 4th 1709, 1718-20 (1994) (burden shift inappropriate where there was no "strong and direct inference of causation [nor did] defendant's negligence absolutely preclude further, definitive proof that the harm to the plaintiff was caused by the defendant's negligence").

Finally, *Smith v. Triad of Alabama, LLC*—the primary support for Plaintiffs' "identity theft losses" model—actually undermines Plaintiffs' arguments and demonstrates precisely why this case cannot proceed as a class action. In *Smith*, a former hospital employee stole medical records with "social security numbers" from "unlocked filing cabinets in a back hallway" and then "dug through the personal information in the patient records and, with the help of an accomplice, filed at least 124 fraudulent federal tax returns for tax years 2012 and 2013." 2017 WL 1044692, at *2. When the police caught the employee, he had "fifty-four patient records in hand." *Id.* Thus, in *Smith*, the evidence established (i) a consistent type of identity theft suffered by the hundreds of class members (tax fraud), (ii) that the necessary information to perpetrate that fraud existed in the stolen records ("social security numbers"), (iii) the identity of the criminal ("Kamarian Millender"), and (iv) proof that Millender committed tax fraud with "at least 124" of the records he stole. *Id.*

Nothing like that exists here. The alleged harms in this case are not consistent across the Named Plaintiffs, but vary widely, including fraudulent payment card charges, fraudulent financial accounts, spam phone calls, spam emails, vanishing emails, collection calls, unwanted pop-up chats, *and* tax fraud. *Supra* at 7. And that is just the Named Plaintiffs. *Id.* The putative class members may (or may not) have experienced other, different harms. Similarly, the information necessary to commit the various crimes or nuisances putative class members may have experienced *may or may not* have been in Yahoo's database or in the putative class member's emails, unlike the Social Security numbers in *Smith*. Finally, unlike *Smith*, where the evidence revealed a single known wrongdoer, here, the wrongdoers are largely unknown. Specifically, Plaintiffs do not allege that the Russian cybercriminals who stole information from Yahoo's user database *themselves* engaged in tax fraud or made spam phone calls, but that these cybercriminals "sold *and resold* that PII on the dark web to *other bad actors*," who Plaintiffs speculate ultimately caused "the harm" they experienced. Mot. at 30 (emphases added). That contention adds an "additional link in the 'causal chain'" and thereby increases the number of individualized inquiries. ECF 132 at 31.

5. Plaintiffs' "Special Relationship" Theory and Demand for Punitive Damages Highlights the Importance of Injury and Causation

Determining whether a given putative class member suffered an injury caused by Yahoo is not only essential to establish liability for all of Plaintiffs' Rule 23(b)(3) sub-classes, it is also fundamental to the calculation of any award of damages (and particularly punitive damages) for at least two reasons.

First, the only reason Plaintiffs can even pursue a claim for damages under a negligence theory is that they successfully pled the "special relationship" exception to the economic loss rule. ECF 215 at 20. But that exception explicitly requires an *individual* analysis of both harm and causation. As this Court explained, there are "six factors for determining when a 'special relationship' exists: '(1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm.'" *Id*. (quoting *J'Aire Corp. v. Gregory*, 598 P.2d 60, 63 (Cal. 1979)).

At least half of these factors are fundamentally incompatible with classwide proof. The foreseeability of harm (factor 2) depends on each individual's unique practices with respect to their PII, and email or other services. That is likely why Plaintiff Essar candidly admitted he had no "special relationship" with Yahoo: Yahoo's database did not have his phone number and his supposed birthday was fake (Ex. 49 (Essar Dep.) at 8:6-7, 242:14-23; Whipple Decl. Ex. 10), and he understood "that no data transmission over the Internet or information storage technology can be guaranteed to be 100 percent secure" such that he was "using Yahoo email at [his] sole risk" (Ex. 49 (Essar Dep.) at 54:9-20). And as explained above, whether a class member suffered an injury (factor 3) and whether there was any "connection" to the attacks (factor 4) each require a detailed individual analysis.

Second, punitive damages, even if warranted, cannot be awarded on a class basis. The Supreme Court has held that due process mandates that the ratio of compensatory to punitive damages "must be based upon the facts and circumstances of the defendant's conduct and the *harm* to the plaintiff." *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 425 (2003) (emphasis added). Accordingly, "courts must ensure that the measure of punishment is both reasonable and proportionate to the *amount of harm to the plaintiff* and to the general damages recovered." *Id.* at 426 (emphasis added). Absent an individual assessment of injury, there can be no reliable proportionality determination.

B. The Paid User and Small Business Sub-Classes Cannot Meet the Requirements of Rule 23

The Paid and Small Business User sub-classes fare no better because they also require individualized inquiries to determine causation and harm. Plaintiffs propose to establish both using "a conjoint analysis to determine the amount of money damage class members overpaid for Defendants' services"—a supposedly security-based sum. Mot. at 27. But that analysis is not admissible, let alone persuasive.

First, Plaintiffs have not provided the Court with a model that actually shows harm—they only proffered an expert who "*proposes*" such a model. Mot. at 27 (emphasis added). That is not good enough. *In re ConAgra Foods, Inc.*, 302 F.R.D. 537, 577 (C.D. Cal. 2014) (holding plaintiffs could not show predominance because "[a]lthough Weir describes the methods he would use to make the calculation—hedonic regression and conjoint analysis—he does not report that he has actually employed them"); *see also Davidson*, 2018 WL 2325426, at *14; *Dolmage*, 2017 WL 1754772, at *7.

Second, Plaintiffs' proposed methodology is unworkable. As the concurrently filed motion to exclude the testimony of Plaintiffs' experts Van Dyke and Parilis ("Van Dyke Mot.") explains, the proposed model violates some of the most basic methodological rules of conjoints and surveys, such as choosing the correct population and not skewing the format and questions to achieve the desired results. *See* Van Dyke Mot. at _. This was no accident: Mr. Van Dyke specifically directed the survey company, Qualtrics, to "always present Yahoo first, prompt to select all that apply" and "to ensure that we have lots of categories that would be expected to bring more security concerns." Ex. 89 (Qualtrics Instructions). Worse, Mr. Van Dyke defined "effective security" as a bundle that contained many features completely unrelated to this case, such as malware protection and spam control (which Yahoo already has). Plaintiffs' conjoint expert Dr. Gary Parilis conceded that survey respondents might choose "security," thinking it meant something other than protection from hackers, and that he would have worded the survey differently in order to capture more accurately the actual concerns of plaintiffs. Ex. 93 (Parilis Dep.) at 170:2–171:8.

Further, California law requires proof of a "specific measure of the amount of [a] loss." *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 330 n.15 (2011). No such measure is available here, because the conjoint analysis cannot determine what proportion of user fees should be apportioned to security for the Paid and Small Business User sub-classes. *See Vaccarino v. Midland Nat. Life Ins. Co.*, 2014 WL 572365, at *9-10 (C.D. Cal. Feb. 3, 2014) (rejecting damages model that did "not compare what [the product] was worth to what plaintiffs paid"); *Chowning v. Kohl's Dept. Stores, Inc.*, 2016 WL

1072129, at *10 (C.D. Cal. Mar. 15, 2016), *aff'd*, 2018 WL 3627741 (9th Cir. Jul. 31, 2018) (focus of restitution analysis is on "what Plaintiff actually received given the price she paid, not on the bargain Plaintiff thought she was receiving"). The conjoint analysis does not "isolat[e] the damages attributable to Defendant's alleged wrongdoing," a necessary prerequisite to demonstrating predominance under *Comcast*. *Werdebaugh*, 2014 WL 7148923, at *11 (citing *Comcast*, 569 U.S. at 35); *see also Bruton v. Gerber Prod. Co.*, 2018 WL 1009257, at *12 (N.D. Cal. Feb. 13, 2018).

Third, even if Plaintiffs had conducted a sound conjoint analysis, they still could not meet their burden at class certification because their theory of harm—that the Paid and Small Business User sub-classes "overpaid for Defendants' service because of the concealed security inadequacies"—is completely unsupported by the evidence. Mot. at 27. At class certification, Plaintiffs must proffer "evidentiary proof." *Comcast*, 569 U.S. at 33; *Guido v. L'Oreal, USA, Inc.*, 2013 WL 3353857, at *14 (C.D. Cal. July 1, 2013) (denying class certification because there was no *evidence* of "a gap" between the prices). They have not—and cannot. The undisputed evidence shows that Yahoo maintained *identical* security measures for paid users and free users. Chhabra Decl. ¶ 14. As Professor Catherine Tucker, an expert in the economics of data privacy explains, because paid users could have received the ***exact same*** security for free, no one can claim to have lost the "benefit of the bargain" when the record is devoid of evidence that there ever was a "bargain." Tucker Rpt. ¶ 240*; see also* ¶¶ 231, 234-36. Just as one cannot recover under the UCL if she "pays $10 for a $10 watch, [she] cannot" recover if she paid "19.95" for a service that was worth "19.95." *Vaccarino*, 2014 WL 572365, at *9-10; *see also Colgan v. Leatherman Tool Grp., Inc.*, 135 Cal. App. 4th 663, 695 (2006) (reversing award of restitution for failure to provide reliable, quantifiable evidence of the value of the alleged lost bargain). The same principles apply to class actions. *See Guido*, 2013 WL 3353857, at *14 (C.D. Cal. July 1, 2013) (denying class certification without prejudice due to the lack of evidence of the quantifiable impact of defendant's alleged misrepresentation on a classwide basis).

Mr. Mortensen's admission that he was not "out of pocket" any money for security is therefore unsurprising: He testified that he paid for his account for three reasons—to avoid advertisements, to synchronize with his other Yahoo account, and to access to customer service. Ex. 60 (Mortensen Dep.)

at 117:12-118:7. And he testified that he was "not seeking *any* financial compensation" from the lawsuit and admitted that "[t]he harm [from a data breach] is of course theoretical, potential" (*id.* at 87:21-22, 250:12-13 (emphasis added)), a fact unchanged by the subsequent qualification that his "attorneys can decide what, if any, settlement is appropriate" (Ex. 61 (Errata Sheet)).

The reality is that the putative class members of the Paid and Small Business User sub-classes are no different from the Free Users. Some may have been harmed by a criminal who committed credit card fraud or identity theft, after seizing upon the fruits of highly sophisticated and state-sponsored attackers who stole PII from Yahoo's database. Tucker Rpt. ¶¶ 50-53. But the vast majority will have suffered no harm, and determining who falls into which bucket cannot be done on a class basis. *Id.*

C. Plaintiffs Cannot Meet the Requirements of Rule 23(b)(2)

Plaintiffs have also sought certification of a class seeking declaratory and injunctive relief under the UCL, including [redacted] Mot. at 19 (citing ECF 252-17 [Frantz Report] at 10-14 [SEALED]). At bottom, Plaintiffs assert that Yahoo's successor, Oath/Verizon, continues to store PII in a fashion that risks further exposure. Mot. at 20. But this proposed class falls far short of the requirements of Rule 23(b)(2).

By its terms, Rule 23(b)(2) certification is appropriate only where "the party opposing the class action has acted or refused to act on grounds generally applicable to the class." The proposed class must be so cohesive that it is appropriate to order the same remedy for all. *Walters v. Reno*, 145 F.3d 1032, 1047 (9th Cir. 1998); *Georgine v. Amchem Prods., Inc.*, 83 F.3d 610 (3d Cir. 1996), *aff'd, Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 624 (1997). Further, to have standing to seek the underlying injunctive relief, Plaintiffs must offer evidentiary proof that they are "immediately in danger of sustaining some direct injury" and the class would all (or mostly all) benefit from the proposed relief. *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983); *see also Chapman v. Pier 1 Imports (U.S.) Inc.*, 631 F.3d 939, 946 (9th Cir. 2011) (en banc) ("[T]o establish standing to pursue injunctive relief ... [plaintiffs] must demonstrate a real and immediate threat of repeated injury in the future."); *Sun Microsystems, Inc. v. Microsoft Corp.*, 188 F.3d 1115, 1123 (9th Cir. 1999) ("Under [the UCL], a plaintiff cannot receive an injunction for past conduct unless he shows that the conduct will probably recur.").

And as Plaintiffs seek Rule 23(b)(2) certification of a UCL claim, they must show that they "suffered injury in fact" *and* "lost money or property *as a result of* the [alleged] unfair competition." Bus. & Prof. Code § 17204 (emphasis added). None of these requirements are satisfied here.

First, the relevant practices at Yahoo have ceased and none of the proposed class representatives here can show through "evidentiary proof" that they have been injured, much less that they are "immediately in danger of sustaining some direct injury" from some hypothetical future attack on Yahoo. Indeed, it is telling that Plaintiffs never even argue, let alone offer evidence, showing that the proposed class representatives face an "immediate threat of future re-injury." *Backhaut v. Apple Inc.*, 2015 WL 4776427, at *8 (N.D. Cal. Aug. 13, 2015) (rejecting (b)(2) certification because the plaintiff failed to show an "immediate threat of future re-injury"). Instead, without *any* evidence, Plaintiffs claim that "Oath still has possession of all of the UCL Injunctive Relief Class members' PII" and the "risk to users of additional intrusions and exfiltration continues unabated." Mot. at 12, 20. That is untrue: there is substantial evidence that many putative class members never stored any actual PII with Yahoo. Whipple Decl. Exs. 11-17; *see also* Chhabra Decl. ¶ 12; *supra* at 4-6. Moreover, putting aside the Forged Cookie attack (which affected none of the Named Plaintiffs), the last attack at issue here occurred almost four years ago. Tepstein Decl. Ex. 5 at 6.

Nor can Plaintiffs credibly claim that Yahoo has ongoing practices that threaten their security now. In *In re Yahoo Mail Litigation*, 308 F.R.D. 577 (N.D. Cal. 2015), in which this Court certified an injunctive relief class, for example, Plaintiffs offered some evidence that Yahoo was continuing to "scan" emails (allegedly without the consent of non-Yahoo users and in violation of California law), thereby establishing, for class certification purposes at least, some alleged ongoing violation of law. *Id*. at 587-88. Here, though, the gravamen of Plaintiffs' complaint is about *past* acts and security practices in connection with the three attacks, which does not "in itself show a present case or controversy regarding injunctive relief . . . if unaccompanied by any continuing, present adverse effects." *O'Shea v. Littleton*, 414 U.S. 488, 495-96 (1974). That is a dispositive difference.

Even if there were ongoing conduct, injunctive relief is appropriate only if there is an *immediate* risk of harm. *See Lyons*, 461 U.S. at 102. None exists here. Plaintiffs Dugas, Essar, and Deana Ridolfo have not produced any evidence that their Yahoo accounts currently contain a significant amount of

PII, and each has testified that they either rarely use their accounts or have stopped using them altogether and do not plan to use them again. Ex. 37 (Dugas Dep.) at 57:13-58:8 ("I don't use my Yahoo accounts anymore"); Ex. 49 (Essar Dep.) at 39:20-25 ("Q. You don't use [the [redacted]] account anymore? A. No. Q. Do you plan to use it in the future? A. No."); 47:4-6 (last time he used the [redacted] account was "[p]robably 10 years ago"); Ex. 77 (D. Ridolfo Dep.) at 37:15-21. Although Ms. Heines identified PII ([redacted]) in her Yahoo email account, that number was not found through an electronic search, but by counsel conducting a "manual search" after hearing Ms. Heines's testimony. Ex. 59. Ms. Ridolfo, for her part, testified that she has not sent any "e-mail out of that Yahoo account in years," that nothing in her Yahoo email is "private and valuable," and that she intends to close her account. Ex. 77 (D. Ridolfo Dep.) at 37:15-21; 41:18-21; 48:23-49:10; 51:5-22; 67:24-68:21. Further, users can stop using Yahoo at any time and delete any emails with PII, as the Yahoo privacy guidelines instruct. Tepstein Decl. Exs. 1-4. There is therefore no reason to believe *any* new information about these plaintiffs will be exposed in the highly speculative event that Yahoo is successfully attacked again. Without a "threat of future re-injury," Plaintiffs cannot establish standing to pursue injunctive relief. *See Backhaut*, 2015 WL 4776427, at *8; *Schulken v. Washington Mut. Bank*, 2012 WL 28099, at *5 (N.D. Cal. Jan. 5, 2012).

Mr. Ridolfo is the *only* proposed class representative who testified he intends to continue to use his Yahoo email. But he too has no "real and immediate threat of repeated injury in the future," *Chapman*, 631 F.3d at 946, because he has admitted there is little chance he will send or receive any PII in his account. Mr. Ridolfo testified that he sent PII through his email on a single occasion, and that it is no longer in his email (assuming it ever was). Ex. 80 (M. Ridolfo Dep.) at 52:20-54:8. And there is no evidence suggesting a plan to send or receive PII in the future, particularly given his stated belief that his single transmission of PII led to the theft of his identity. *See id.* at 88:19-89:21 (noting that he deleted sensitive information sent through his email after someone stole his identity); 94:9-95:5 (same); 103:7-11 (same). Thus, Mr. Ridolfo cannot claim to be "immediately in danger of sustaining some direct injury" either. *Lyons*, 461 U.S. at 102.

Second, Plaintiffs Dugas and Heines also lack standing under the UCL. As this Court has twice held, the "risk of future costs as a result of the Data Breaches . . . is not sufficient to allege 'lost money or property' under the UCL." ECF 132 at 39; ECF 215 at 16; *see also In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim because plaintiffs failed to allege that they lost money or property, even where plaintiffs alleged the dissemination of personal information and the lost sales value of that information); *In re iPhone Application Litig.*, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) ("Numerous courts have held that a plaintiff's 'personal information' does not constitute money or property under the UCL."). While Dugas and Heines allege having lost money or property, the *evidence* demonstrates that the tax fraud that Dugas suffered and the debit card fraud that Heines suffered have no plausible connection to the attacks on Yahoo. Ferrante Rpt. at 25-26, 29-32. Thus, they cannot show that they "personally 'lost money or property *as a result* of the [alleged] unfair competition.'" ECF 215 at 15 (quoting Cal. Bus. & Prof. Code § 17204 and citing *Kwikset Corp. v. Superior Court*, 246 P.3d 877, 887 (Cal. 2011)) (emphasis added).

Third, even if Plaintiffs could seek prospective relief, (b)(2) certification would be inappropriate because they failed "to carry their burden of showing such [injunctive] relief is plausible." *Vallario v. Vandehey*, 554 F.3d 1259, 1267-68 (10th Cir. 2009). As support for their proposed injunction, Plaintiffs rely *entirely* on the recommendations from their security expert, Mary Frantz. Mot. at 19. But as explained in the accompanying motion to exclude her testimony ("Frantz Mot."), Ms. Frantz's recommendations are inadmissible. Without them, Plaintiffs cannot "describe[] in reasonably particular detail" their requested relief, "such that the court can at least conceive of an injunction that would satisfy [Rule 65(d)'s] requirements," much less provide the evidentiary support necessary to satisfy Rule 23(b)(2). *Shook v. Bd. of Cty. Comm'rs of Cty. of El Paso*, 543 F.3d 597, 605-06 (10th Cir. 2008) (affirming denial of (b)(2) certification) (internal quotations omitted); *see also Parsons v. Ryan*, 289 F.R.D. 513, 524 (D. Ariz. 2013), *aff'd*, 754 F.3d 657 (9th Cir. 2014); *Vallario*, 554 F.3d at 1267-68.

Even if the Court does not exclude Ms. Frantz's recommendations, the injunctive measures she describes are inappropriate because they are overbroad and largely "dissociated from" Yahoo's alleged acts. *See, e.g.*, *N.L.R.B. v. Express Pub. Co.*, 312 U.S. 426, 435-36 (1941); *see also A.A. v. Cty. of Riverside*, 2017 WL 5624296, at *14 (C.D. Cal. Nov. 7, 2017) (injunctive relief class failed under Rule 23(b)(2) in part because of lack of evidence showing defendants were actually doing what the injunction sought to prevent). For example, Ms. Frantz contends that Oath should become [redacted] [redacted]" and [redacted]" (ECF 252-17 at 11), but that form of certification applies only to government agencies and contractors, which Yahoo is not (Frantz Mot. at 3-4). Additionally, Ms. Frantz admitted that her recommendations were based on events from 2008 to 2016. Much of that timeline involves events other than the 2013, 2014, and Forged Cookie attacks. *Id.* at 4. In fact, Ms. Frantz testified that her recommendations were an afterthought, added to her report "at the last minute," and were merely off-the-shelf suggestions for how Yahoo could improve its "security posture" generally. *Id.*; Ex. 95 (Frantz Dep.) at 109:16-113:7. Because it would force Yahoo to take actions "far beyond the bounds of this lawsuit" (*Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 518 F. Supp. 2d 1197, 1226 (C.D. Cal. 2007)), Plaintiffs' proposed injunctive relief cannot serve as a basis for Rule 23(b)(2) certification.

D. Plaintiffs Cannot Meet the Requirements of Rule 23(c)(4)

Plaintiffs' last-ditch request for issue certification under Rule 23(c)(4) in the event "the Court ultimately finds fault with Plaintiffs' models on an aggregate level" is meritless. They seek to justify such certification based on the same erroneous assumption that "common PII [was] taken from all Damages Class members." Mot. at 35. But the evidence demonstrates the exact opposite: whether a class member had PII exposed in the attacks, and if so what kind of PII, varies from person to person.

In any event, certifying a class under Rule 23(c)(4) is inappropriate because it will not "significantly advance the resolution of the underlying case." *Valentino,* 97 F.3d at 1229. As this Court recently explained, it does not make sense to certify issues under Rule 23(c)(4) when "the ultimate question of [the defendant's] liability . . . would still have to be resolved on an individual basis." *Davidson*, 2018 WL 2325426, at *26; *see also Huu Nguyen v. Nissan N. Am., Inc.*, 2018 WL 1831857, at *8 (N.D. Cal. Apr. 9, 2018) (rejecting Rule 23(c)(4) certification where it would not materially "advance the litigation"); *Backhaut*, 2015 WL 4776427, at *3 n.3 (similar); *Werdebaugh*, 2014 WL 7148923, at *14 n.9 (similar). Here, even if the Court were to grant Plaintiffs' (c)(4) motion in full, and even if Plaintiffs prevailed on *every* issue, the factfinder still could not award a penny to any class member until that class member came to court, subjected himself or herself to discovery, and proved that he or she suffered compensable harm as a result of the attacks.

Further, a Rule 23(c)(4) class is impermissible as a matter of law as a "stand-alone" class—it must be paired with a properly certified class under one of the Rule 23(b) subsections. As the Supreme Court has explained, the party seeking certification must prove that (1) Rule 23(a)'s requirements have been met, *and* (2) that "*the proposed class must satisfy at least one of the three requirements listed in Rule 23(b)*." *Dukes*, 564 U.S. at 345 (emphasis added). "[A] class action movant cannot gerrymander predominance by" slicing and dicing the case to exclude "other individualized issues [that] will dominate or be meaningfully material to the resolution of the absent class members' claims." *Hamilton v. O'Connor Chevrolet, Inc.*, 2006 WL 1697171, at *6 (N.D. Ill. June 12, 2006) (citing *Castano v. Am. Tobacco Co.*, 84 F.3d 734, 745 n.21 (5th Cir. 1996)).[8] There is no certifiable (c)(4) issue here.

E. Plaintiffs Cannot Bring Claims Related to the Forged Cookie Attack

Finally, Plaintiffs cannot bring claims related to the Forged Cookie attack because no class representative has provided evidence to support their allegations that they were affected, much less injured, by that attack. In particular, there is no evidence any received a notice their accounts were affected by that attack, and Yahoo's records confirm they were not. Chhabra Decl. ¶ 3. Accordingly, Plaintiffs lack an adequate representative for claims related to the Forged Cookie attack. *See Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 158 (1982).

IV. Conclusion

For the foregoing reasons, Plaintiffs cannot satisfy any of the requirements for Rule 23(b)(2), (b)(3), or (c)(4) certification. Accordingly, the Court should deny their motion for class certification.

Dated: August 31, 2018

GIBSON, DUNN & CRUTCHER LLP

By: /s/ *Theodore J. Boutrous, Jr.*
Theodore J. Boutrous, Jr.

Attorneys for Defendants YAHOO! INC. and
AABACO SMALL BUSINESS, LLC

[8] To the extent *Valentino v. Carter-Wallace, Inc.* suggests otherwise, it has been abrogated by the Supreme Court's clear statement to the contrary in *Dukes*.